



①9 BUNDESREPUBLIK  
DEUTSCHLAND



DEUTSCHES  
PATENT- UND  
MARKENAMT

⑫ **Offenlegungsschrift**  
⑩ **DE 100 52 312 A 1**

⑤ Int. Cl.<sup>7</sup>:  
**H 04 L 12/28**  
H 04 L 12/22  
H 04 L 12/56  
G 06 F 12/14

⑲ Aktenzeichen: 100 52 312.9  
⑳ Anmeldetag: 21. 10. 2000  
㉓ Offenlegungstag: 8. 11. 2001

DE 100 52 312 A 1

③0 Unionspriorität:  
428400 28. 10. 1999 US

⑦1 Anmelder:  
International Business Machines Corporation,  
Armonk, N.Y., US

⑦4 Vertreter:  
Duscher, R., Dipl.-Phys. Dr.rer.nat., Pat.-Ass., 71034  
Böblingen

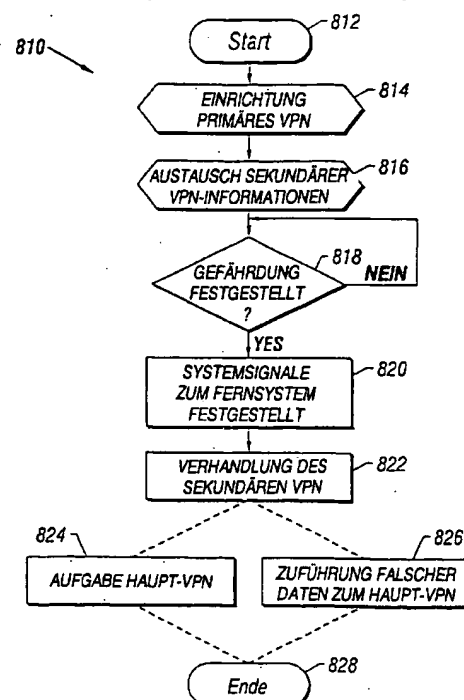
⑦2 Erfinder:  
Genty, Denise Marie, Austin, Tex., US; McBrearty,  
Gerald Francis, Austin, Tex., US; Mullen, Shawn  
Patrick, Buda, Tex., US; Shieh, Johnny Meng-Han,  
Austin, Tex., US; Unnikrishnan, Ramachandran,  
Austin, Tex., US

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

⑤4 Automatische Sperre gegen unberechtigten Zugriff im Internet (Snoop Avider) für virtuelle private Netze

⑤7 Offengelegt werden ein System und ein Verfahren zur Verbesserung der Sicherheit von Verbindungen eines virtuellen privaten Netzes (VPN) durch automatische Vorverhandlungen einer zweiten Konfiguration. Wenn unberechtigte Zugriffe oder andere Sicherheitsverstöße festgestellt werden, wird der VPN-Tunnel automatisch zu einer zweiten vorbereiteten Konfiguration hin verändert, um so die versuchten Sicherheitsverletzungen zu vereiteln.



DE 100 52 312 A 1



## Beschreibung

## Querverweis auf zugrunde liegende Anmeldung

[0001] Die vorliegende Anmeldung bezieht sich auf die gleichzeitig eingereichte US-Patentanmeldung mit der Seriennummer 09/428,401 (Attorney Docket No. AT 9-99-351) mit dem Titel "Manual Virtual Private Networking Internet Snooper Avoider".

## Technisches Gebiet

[0002] Die vorliegende Erfindung bezieht sich im Allgemeinen auf Datenverarbeitungsnetzsysteme und insbesondere auf virtuelle private Netze (virtual private network, VPN); die Tunnelungs- oder Kapselungsverfahren verwenden.

## HINTERGRUNDINFORMATIONEN

[0003] Ein virtuelles privates Netz ist eine Erweiterung eines privaten Intranet-Netzes über ein öffentliches Netz, wie beispielsweise das Internet, um eine sichere private Verbindung herzustellen. Dieser Effekt wird, wie nachfolgend beschrieben, durch einen verschlüsselten privaten Tunnel erreicht. Ein VPN transportiert Informationen sicher über das Internet und verbindet ferne Benutzer, Zweigstellen und Geschäftspartner zu einem erweiterten Verbundnetz.

[0004] Tunnelung oder Kapselung ist eine gängige Technik für paketvermittelte Netze. Ein Paket eines ersten Protokolls wird in einem zweiten Paket eines zweiten Protokolls "verpackt". Dazu wird ein neuer Header eines zweiten Protokolls dem ersten Protokoll hinzugefügt. Das zweite Paket enthält nun die Nutzinformation des ganzen ersten Pakets. Die Tunnelung wird oft verwendet, um den Datenverkehr eines Protokolls über ein Netz zu transportieren, das dieses Protokoll nicht direkt unterstützt. Zum Beispiel kann ein NetBIOS-Paket (Network Basic Input/Output System) oder ein IPX-Paket (Internet Packet Exchange) in ein IP-Paket (Internet Protocol) eingebunden werden, um über ein TCP/IP-Netz (Transmission Control Protocol/Internet Protocol) transportiert zu werden. Wenn das erste eingebundene Paket verschlüsselt ist, wird ein Eindringling oder Hacker Probleme haben, die wahre Zieladresse und den Dateninhalt des ersten Pakets herauszufinden.

[0005] Die Verwendung von virtuellen privaten Netzen wirft einige Sicherheitsbedenken auf, die über die bereits in traditionellen firmeneigenen Intranet-Netzen vorhandenen Bedenken hinausgehen. Ein typischer Endpunkt-zu-Endpunkt-Datenpfad kann einige Maschinen umfassen, die nicht unter der Kontrolle der Firma stehen, wie beispielsweise den Zugangscomputer des Internet Service Providers (Internet-Dienstanbieter), ein Einwahlsegment oder die Router (Wegewähler) innerhalb des Internets. Der Pfad kann auch ein Sicherheits-Gateway (Sicherheitsübergang), wie zum Beispiel eine Firewall (Brandmauer) oder einen Router, beinhalten, das sich am Übergang eines internen Segments und eines externen Segments befindet. Der Datenpfad kann auch ein internes Segment beinhalten, das als Host oder Router dient und eine Mischung von innerbetrieblichem und zwischenbetrieblichem Datenverkehr transportiert. Die Datenpfade beinhalten üblicherweise externe Segmente wie das Internet, die nicht nur Daten aus dem Verbundnetz sondern auch von anderen Quellen transportieren.

[0006] In dieser heterogenen Umgebung gibt es viele Möglichkeiten zu lauschen, Inhalte von Datenpaketen zu verändern, Denial-of-Service-Attacken (Netzdienst-Sabotage) zu betreiben oder die Zieladresse eines Datenpakets

zu verändern. Gegenwärtige Verschlüsselungsalgorithmen sind nicht perfekt und sogar verschlüsselte Datenpakete können gelesen werden, wenn ausreichend Zeit vorhanden ist. Die Verwendung eines virtuellen privaten Netzes innerhalb dieser Umgebung gibt solchen potentiellen Eindringlingen und Hackern ein festes Ziel vor, da sich weder die Endpunkte des virtuellen privaten Netzes noch die Verschlüsselungsverfahren und Chiffrierschlüssel verändern. Die vorliegende Erfindung bezieht sich auf die Sicherheitsbedenken, die dieses System beinhaltet.

## ÜBERBLICK ÜBER DIE ERFINDUNG

[0007] Die vorliegende Erfindung umfasst eine Vorrichtung und ein Verfahren für die Vorverhandlung und die teilweise zufällige Erzeugung einer zweiten Konfiguration eines virtuellen privaten Netzes oder eines anderen getunnelten Netzes, für den Fall, dass die Sicherheit des Haupt-VPN gefährdet wird. Konfigurationseigenschaften, wie Quell- und Zieladressen der Knoten, deren Chiffrierschlüssel und Verschlüsselungsalgorithmen, werden üblicherweise ausgetauscht, um ein Haupt-VPN oder ein getunneltes Netz einzurichten. Wenn eine Gefährdung des Haupt-VPN oder des getunnelten Netzes erwartet wird, werden in der vorliegenden Erfindung ein Satz verwendbarer Adressen sowie verwendbare Verschlüsselungsverfahren zusammen mit zufallsgenerierten Chiffrierschlüsseln zwischen den Knoten ausgetauscht. Die getunnelten Knoten sind so konfiguriert, dass im Fall einer Feststellung einer Gefährdung oder einer versuchten Gefährdung des Haupt-VPN eines der möglichen sekundären virtuellen privaten Netze, die durch diese sekundären Konfigurationen repräsentiert werden, genutzt werden kann.

[0008] Eine Gefährdung des VPN oder getunnelten Netzes kann durch eines der zahlreichen, nach dem Stand der Technik bekannten Mittel festgestellt werden, beispielsweise durch einen Alert (Warnhinweis) vom Server. In der Vorliegenden Erfindung können die sekundären Konfigurationen, die zwischen den Knoten ausgetauscht werden, automatisch verwendet werden, um ein zweites VPN oder ein zweites getunneltes Netz aufzubauen, wenn das Haupt-VPN oder das getunnelte Netz nicht mehr verwendet wird oder falsche Daten zugeführt werden.

[0009] Die bereits erwähnten Erklärungen beschreiben in groben Zügen die Eigenschaften und die technischen Vorteile der vorliegenden Erfindung, um die nachfolgenden ausführlichen Erläuterungen der Erfindung besser verständlich zu machen. Zusätzliche Eigenschaften und technische Vorteile der Erfindung, die Gegenstand der Patentansprüche der Erfindung sind, werden nachfolgend beschrieben.

## KURZBESCHREIBUNG DER ZEICHNUNGEN

[0010] Zum besseren Verständnis der vorliegenden Erfindung und der daraus folgenden Vorteile wird nun Bezug genommen auf die nachfolgenden Beschreibungen zusammen mit den begleitenden Zeichnungen, wobei:

[0011] Fig. 1 ein Übersichtsblockdiagramm eines VPN-Systems darstellt;

[0012] Fig. 2 ein Blockdiagramm eines Pakets innerhalb eines VPN oder eines getunnelten Netzprotokolls darstellt;

[0013] Fig. 3 ein Blockdiagramm eines Computers innerhalb eines VPN-Netzsystems darstellt;

[0014] Fig. 4 ein Diagramm zur Veranschaulichung des Zusammenhangs von IP-Adressen, Chiffrierschlüsseln und Verschlüsselungsverfahren innerhalb eines VPN-Systems darstellt;

[0015] Fig. 5 ein Diagramm zur Veranschaulichung des



Zusammenhangs von IP-Adressen, Chiffrierschlüsseln und Verschlüsselungsverfahren innerhalb eines VPN-Systems ist, das eine Änderung des VPN-Systems durch die vorliegende Erfindung demonstriert;

[0016] Fig. 6A ein Diagramm zur Veranschaulichung der Rotation in der Anwendung eines Satzes verfügbarer IP-Adressen durch die vorliegende Erfindung ist;

[0017] Fig. 6B ein Diagramm zur Veranschaulichung der Rotation in der Anwendung eines Satzes verfügbarer Chiffrierschlüssel durch die vorliegende Erfindung ist;

[0018] Fig. 6C ein Diagramm zur Veranschaulichung der Rotation in der Anwendung eines Satzes verfügbarer Verschlüsselungsalgorithmen durch die vorliegende Erfindung ist;

[0019] Fig. 7 ein Übersichtsblockdiagramm eines VPN-Systems darstellt, wobei sich bei einem der Knoten ein Haupt- und ein sekundärer VPN-Tunnel im Betrieb befinden;

[0020] Fig. 8 ein Flussdiagramm gemäß dem ANSI/ISO Standard 5807-1985 darstellt, das die Vorgehensweise der vorliegenden Erfindung beschreibt.

#### AUSFÜHRLICHE BESCHREIBUNG DER ERFINDUNG

[0021] In der nachfolgenden Beschreibung werden zahlreiche spezifische Details erklärt, wie das Protokoll der Netzübertragung, die Bytelänge, die Adressen, etc., um ein umfassendes Verständnis der Erfindung zu gewährleisten. Für Fachleute ist es jedoch offensichtlich, dass die vorliegende Erfindung auch ohne diese spezifischen Details realisiert werden kann. In anderen Fällen wurden wohlbekannte Schaltkreise, Computerausrüstungen oder Netzeinrichtungen in Form von Blockdiagrammen dargestellt, um die vorliegende Erfindung nicht mit unnötigen Details zu überladen. Meist wurden Details bezüglich Taktung, verwendeter spezifischer Ausrüstung und Programmiersprachen, verwendeter Verschlüsselungsverfahren und dergleichen weggelassen, sofern diese Details nicht notwendig sind, um ein vollständiges Verständnis der vorliegenden Erfindung zu erhalten, und im Rahmen der üblichen Kenntnisse von Fachleuten liegen.

[0022] Im Rahmen dieser Beschreibung ist beabsichtigt, dass der Begriff "Knoten" eine Verarbeitungsmaschine, z. B. einen Computer, oder eine Gruppe von Verarbeitungsmaschinen oder Computern, wie z. B. ein lokales Netz (local area network, LAN) oder ein Weitverkehrsnetz (wide area network, WAN), die elektrisch mit einem Netzsystem verbunden sind, umfasst. Folglich kann ein "Knoten", wie er im vorliegenden Dokument verwendet wird, ein LAN von Computern mit einem Gateway oder ein WAN von LANs mit mehreren Gateways und Routern umfassen. Es ist beabsichtigt, dass die beschriebenen und zugeschriebenen Verarbeitungseigenschaften eines Knotens demnach von einem einzelnen Computer, einem oder mehreren Computern, von Gateways oder Routern innerhalb eines LAN oder von einem oder mehreren Computern, Gateways oder Routern innerhalb eines WAN erfüllt werden. Im Rahmen dieses Patents wird mit dem Begriff "VPN" ein virtuelles privates Netz (virtual private network) oder ein anderes beliebiges eingebundenes oder getunneltes Netzprotokoll bezeichnet.

[0023] Fig. 1 zeigt ein VPN-System 108. Ein Intranet 110 ist ein System von Netzcomputern mit einer Organisation, die ein oder mehrere Netzprotokolle für die Kommunikation verwendet. Ein Intranet 110 kann ein oder mehrere lokale Netze (LAN), Weitverkehrsnetze (WAN) oder eine Kombination aus beiden umfassen. Oft muss ein Verbund-Intranet (associate intranet) 112 mit dem Intranet 110 verbunden werden. Ein Verbund-Intranet 112 kann ein Geschäftspart-

ner, Lieferant oder eine Zweigstelle sein. Das Verbund-Intranet 112 kann auch LANs, WANs oder eine Kombination aus beiden umfassen. Eine Einzelperson könnte auch einen Fernzugriff über eine Fernzugriffsmaschine 114 zum Intranet 110 benötigen.

[0024] Für den Fall, dass das Verbund-Intranet 112 oder die Fernzugriffsmaschine 114 nicht direkt mit dem Internet 110 verbunden sind, kann bei der Konfiguration eines Systems das Intranet 110 mittels Internet 116 mit dem Verbund-Intranet 112 und der Fernzugriffsmaschine 114 verbunden werden. In einem solchen Fall werden, alle, das Intranet 110, das Verbund-Intranet 112 und die Fernzugriffsmaschine 114, zu Knoten im Internet 116.

[0025] Es wird in Fachkreisen gern gesehen, wenn das Internet 116 aus einer Reihe von Maschinen besteht, die mittels eines TCP/IP-Netzprotokolls zu einem Netz verbunden sind. Obwohl das TCP/IP-Netz ein universelles Protokoll darstellt, das die Verbindung vieler verschiedener Maschinen zum Internet 116 ermöglicht, wirft es zahlreiche Sicherheitsfragen auf. Übertragungen über das Internet 116 sind nicht sicher und können Ziele von Lauschangriffen (eavesdropping), Denial-of-Service-Attacken, unberechtigten Zugriffen und einer Auswahl anderer Sicherheitsverstöße werden. Folglich ist die Übertragung sehr sensibler Daten über das Internet 116 ohne Sicherheitsmaßnahmen in Form von Verschlüsselung allgemein als unsicher erkannt worden. Die Sicherheitsbedenken wachsen, wenn stetige und systematische Übertragungen über das Internet 116 durchgeführt werden, wie beispielsweise die, welche erforderlich sind, um eine Netzverbindung zwischen dem Intranet 110 und dem Verbund-Intranet 112 oder der Fernzugriffsmaschine 114 aufrechtzuerhalten.

[0026] Fachleute werden das virtuelle private Netz als eine Teillösung dieser Probleme, die es gegenwärtig nach dem Stand der Technik gibt, erkennen. Ein VPN-Tunnel 118 kann zwischen dem Intranet 110 und dem Verbund-Intranet 112 oder der Fernzugriffsmaschine 114 definiert werden. Jede der Komponenten – Intranet 110, Verbund-Intranet 112 und Fernzugriffsmaschine 114 – wird dann, ebenso wie das Internet 116, zum Knoten im VPN-Tunnel. Der VPN-Tunnel 118 stellt eine Verschlüsselungseinrichtung über das Internet 116 zur Verfügung, die die Daten zwischen dem Intranet 110 und dem Verbund-Intranet 112 oder der Fernzugriffsmaschine 114 durchlaufen können.

[0027] Fig. 2 stellt ein eingebundenes Paket zur Übertragung über den VPN-Tunnel 118 und ein Intranet-Paket 112 dar, das aus einem IP-Header 214 und einer Nutzinformation 216 besteht. Der IP-Header 214 ist typisch für ein TCP/IP-Protokoll, aber Fachleute erkennen, dass eine solche Kapselungstechnik oft in anderen Netzprotokollen auf diesem Gebiet verwendet wird. Der IP-Header 214 enthält Informationen, wie die Adresse der Quellmaschine, die Adresse der Zielmaschine sowie andere Verwaltungsdaten. Auf der anderen Seite enthält die Nutzinformation 216 die Daten, die von der Quellmaschine zur Zielmaschine übertragen werden sollen. In einem VPN-System wird dem Originalpaket 212 ein neuer IP-Header 218 vorangestellt. Der neue IP-Header 218 enthält die gleiche Art von Verwaltungsinformationen wie der IP-Header 214, jedoch veranlassen die Verwaltungsinformationen im neuen IP-Header 218, dass das ganze Paket zum Endpunkt des VPN-Tunnels 118 transportiert wird. Oft wird das ganze eingebundene Paket 212 vor dem Anhängen des neuen IP-Headers 218 verschlüsselt. Auf diese Weise kann die Partei, die das getunnelte Paket abfängt, nicht ohne weiteres Informationen aus dem Originalpaket 212 entnehmen.

[0028] Eine typische Hardware-Umgebung zur Anwendung der vorliegenden Erfindung ist in Fig. 3 abgebildet, die



eine typische Hardwarekonfiguration eines Datenverarbeitungssystems **313** gemäß dem Gegenstand der Erfindung darstellt, das eine Zentraleinheit (central processing unit, CPU) **310**, z. B. einen konventionellen Mikroprozessor, und eine Anzahl anderer durch einen Systembus **312** miteinander verbundener Einheiten aufweist. Das System **313** beinhaltet einen Speicher **314**, der aus einem Arbeitsspeicher (random access memory, RAM) und einem Festspeicher (read only memory, ROM) besteht. Das System **313** umfasst auch einen Ein-/Ausgabe-Adapter (input/output adapter, I/O) **318** zum Anschluss peripherer Geräte, wie Platteneinheiten **320**, am Bus **312**, eine Benutzerschnittstelle **322** zum Anschluss einer Tastatur, einer Maus und/oder anderer Benutzerschnittstellengeräte (nicht abgebildet), am Bus **312**, einen Kommunikationsadapter **334** zum Anschluss des Systems **313** an ein Datenverarbeitungsnetz, wie beispielsweise ein LAN und/oder ein WAN. Das System **313** kann auch eine Anzeigeeinheit **336** zum Anschließen eines Anzeigegeätes (nicht abgebildet) an den Bus **312** umfassen. Die Zentraleinheit **310** kann auch andere, hier nicht abgebildete Schaltungen umfassen, die in einem Mikroprozessor üblichen Schaltungen enthalten. Das System **315** kann auch an jedem der bereits erwähnten Knoten verwendet werden.

[0029] Der Kommunikationsadapter **334** ist so angepasst, dass Daten vom Bus **312** empfangen und zur Übertragung über das Netz **340** an ein Netzwerkprotokoll angepasst werden. Ein solches Protokoll kann TCP/IP, NetBIOS oder eine Vielfalt anderer Netzwerkprotokolle sein, die nach dem Stand der Technik üblich sind. Der Kommunikationsadapter **334** verfügt über eine oder mehrere mit ihm verbundene Adressen, die verwendet werden können, um ausgehende Pakete zu "kennzeichnen" oder festzustellen, ob ein eingehendes Paket für ihn bestimmt ist. Der Kommunikationsadapter **334** kann auch eine "Aliasnamensprüfung" vornehmen, um gleichzeitig mehr als eine Adresse diesem Kommunikationsadapter **334** zuzuordnen. Die zu übertragenden Informationen werden zur oben in Fig. 2 erklärten Nutzinformation **216**. Der Kommunikationsadapter **334** kann auch angepasst werden, um Daten vom Netz **340** zu empfangen und diese als Nutzinformation **216** eines eingebundenen Pakets umzupacken oder weiterzuleiten.

[0030] Die Arbeitsweise der vorliegenden Erfindung ist in Fig. 4 dargestellt. Eine Intranet-Struktur **410** kann mehrere VPN-Tunnelverbindungen **412**, **414** aufweisen. Jeder der VPN-Tunnelverbindungen **412**, **414** ist eine IP-Adresse **430**, ein Chiffrierschlüssel **432** und ein Verschlüsselungsverfahren **434** zugeordnet. Wie nach dem Stand der Technik üblich, ist die IP-Adresse **430** eine eindeutige Adresse innerhalb des Internets **116**, wie Fig. 1 zeigt.

[0031] Der Chiffrierschlüssel **432** und das Verschlüsselungsverfahren **434** können eine beliebige Anzahl von Schlüsseln oder Verfahren sein, wie es in der Computerver- schlüsselungstechnik festgelegt ist. Eine Vielzahl von Verschlüsselungsverfahren stehen zur Verfügung, die eine Vielzahl von Chiffrierschlüsseln **432** verschiedenen Umfangs verwenden, sodass jede Maschine ihren eigenen Chiffrierschlüssel **432** hat. Üblich sind 128-Bit-Schlüssel. Der Chiffrierschlüssel **432** ermöglicht der Intranet-Struktur **410**, gesendete und empfangene Pakete zu verschlüsseln und zu entschlüsseln, wenn er unter Anwendung des Verschlüsselungsverfahrens **434** verwendet wird. Ein Vorteil der vorliegenden Erfindung besteht darin, dass sie von den Chiffrierschlüsseln **432** und den Verschlüsselungsverfahren **434** unabhängig ist, sodass mit der vorliegenden Erfindung jedes beliebige Verschlüsselungsverfahren mit beliebig vielen Chiffrierschlüsseln verwendet werden kann.

[0032] In Fig. 4 sind Strukturen eines Verbund-Intranets **432** abgebildet, die jeweils eine zugeordnete IP-Adresse, ei-

nen Chiffrierschlüssel und ein Verschlüsselungsverfahren aufweisen, wodurch die VPN-Tunnelverbindung **420** festgelegt wird. Eine Fernzugriffsstruktur **430** hat ebenfalls eine zugeordnete VPN-Tunnelverbindung **418**, die die gleichen Konfigurationsinformationen aufweist. Die Verbund-VPN-Tunnelverbindungen **420** und die VPN-Tunnelverbindungen **414** legen einen VPN-Tunnel **428** fest. Die VPN-Tunnelverbindung **418** und die VPN-Tunnelverbindung **412** legen ebenfalls einen VPN-Tunnel **428** fest.

[0033] Die vorliegende Erfindung beinhaltet den Austausch von Elementen einer sekundären VPN-Konfiguration, wie IP-Adresse, Chiffrierschlüssel und Verschlüsselungsverfahren, zwischen einer Intranet-Struktur **410** und einer Fernzugriffsmaschine **418** oder einem Verbund-Intranet **420** unmittelbar nach der Einrichtung eines VPN-Tunnels **428**, **426**.

[0034] Weil Adressen typischerweise eindeutig sein müssen, tauschen die Maschinen mindestens eine sekundäre Adresse, optimalerweise aber einen Satz von Adressen aus, die dieser Maschine zugewiesen sind oder zugewiesen werden können. Der von jeder Maschine unterstützte Satz von Verschlüsselungsverfahren ist ebenfalls ein fester Satz, sodass dieser unterstützte Satz von Verschlüsselungsverfahren ausgetauscht wird. Schließlich wird auch ein zufallsgenerierter Schlüssel für jedes Verschlüsselungsverfahren ausgetauscht.

[0035] Einmal ausgetauscht, werden die sekundären Konfigurationselemente für die Fernzugriffsmaschine **418** durch die Intranet-Struktur **410** gespeichert. Die sekundären Konfigurationselemente der Intranet-Struktur **410** werden ebenfalls auf der Fernzugriffsmaschine **418** gespeichert.

[0036] In dem Fall, dass entweder die Intranet-Struktur **410** oder die Fernzugriffsmaschine **418** unberechtigte Zugriffe oder andere mögliche Sicherheitsverstöße entlang des VPN-Tunnels **428** feststellt, wird die feststellende Maschine einen vordefinierten Verwaltungsänderungscode an die andere Maschine übermitteln. Der Änderungscode gibt an, welche von den vorher ausgetauschten sekundären Konfigurationselementen verwendet werden müssen. Da die Sicherheit des VPN-Tunnels **428** bereits gefährdet sein kann, darf der Änderungscode nicht die aktuellen sekundären Konfigurationselemente beinhalten. Vielmehr muss der Änderungscode einen Code benennen, der symbolisiert, welche sekundären Konfigurationselemente verwendet werden müssen.

[0037] Eine Ausführungsart des Verfahrens der vorliegenden Erfindung ist in Fig. 8 dargestellt. Ein Änderungsalgorithmus **810** beginnt bei Schritt **812** mit der Vorbedingung des Vorhandenseins eines Netzsystems. Ein primärer VPN-Tunnel zwischen zwei Knoten des Netzsystems wird in Schritt **814** eingerichtet. Danach tauschen die Knoten in Schritt **816** sekundäre VPN-Konfigurationsinformationen aus. Ein solcher Austausch kann über den zuvor in Schritt **814** eingerichteten primären VPN-Tunnel erfolgen. Der Algorithmus **810** wartet dann, bis eine Gefährdung in Schritt **818** festgestellt wird. Wie bereits erwähnt, kann eine Gefährdung entweder ein Sicherheitsverstoß oder eine technische Störung sein. Liegt eine Gefährdung vor, übermittelt der feststellende Knoten dem Fernknoten den Verwaltungsänderungscode in Schritt **820**. Daraufhin verhandeln beide, der feststellende Knoten und der Fernknoten, in Schritt **822** automatisch einen sekundären VPN-Tunnel.

[0038] Nach der Einrichtung des sekundären VPN-Tunnels in Schritt **822** kann der Algorithmus **810** entweder das Aufgeben des primären VPN-Tunnels in Schritt **824** oder die Einspeisung falscher Daten in den primären VPN-Tunnel in Schritt **826** veranlassen. Der Algorithmus kann in Schritt **828**, wie gezeigt, beendet werden, oder in einer alter-



nativen Ausführung in einer Schleife zusätzliche VPN-Informationen in Schritt 816 austauschen.

[0039] Fig. 5 zeigt ein mögliches Ergebnis eines Verwaltungsänderungscodes. Die Intranet-Struktur 510 hat das Ende des sekundären VPN-Tunnels 528 in Übereinstimmung mit der sekundären Konfigurationsinformationen 512 neu konfiguriert. Die Fernzugriffsmaschine 518 hat ebenfalls anhand der VPN-Konfigurationsinformationen, die ihr durch die Intranet-Struktur 510 vorher gesendet wurden, neu konfiguriert. Als Ergebnis gibt es nun den sekundären VPN-Tunnel 528 zwischen zwei verschiedenen IP-Adressen mit verschiedenen Chiffrierschlüsseln und einem anderen Verschlüsselungsverfahren. Alle Versuche, die Sicherheit des ursprünglichen VPN-Tunnels 428 zu gefährden, werden vereitelt.

[0040] Fig. 7 zeigt die Anordnung des VPN-Systems 708 nach der Inbetriebnahme des sekundären VPN-Tunnels 720. Der ursprüngliche VPN-Tunnel 718 ist zu diesem Zeitpunkt noch aktiv. Wegen seiner Gefährdung sollte jedoch der ursprüngliche VPN-Tunnel 718 nicht für die Übertragung zwischen dem Intranet 710 und der Fernzugriffsmaschine 714 verwendet werden.

[0041] Nach der Einrichtung des sekundären VPN-Tunnels 720 kann der ursprüngliche VPN-Tunnel 718 aufgegeben oder mit falschen Daten versorgt werden. Es ist von Vorteil, dass ein einziger VPN-Tunnel geändert werden kann, ohne andere VPN-Tunnel innerhalb des gleichen Systems 708 zu verändern.

[0042] Die sekundären Konfigurationselemente können durch die Maschine, die einen Änderungscode sendet, anhand einer beliebigen Anzahl von Algorithmen ausgewählt werden, und es ist von Vorteil, dass viele Variationen das im vorliegenden Dokument vorgestellten Verfahrens möglich und anhand dieser Offenlegung offensichtlich sind. De facto verbessern die fast unendlichen Möglichkeiten verschiedener Auswahlalgorithmen die Sicherheit.

[0043] Ein möglicher Algorithmus zur Auswahl von Adressen ist in Fig. 6A gezeigt. Eine VPN-Hauptadresse 610 wird zusammen mit einer ersten sekundären Adresse 612, einigen zusätzlichen sekundären Adressen 616 und einer endgültigen sekundären Adresse 614 angefordert. Der VPN-Hauptadresse 610 ist auch ein VPN-Hauptadresscode 620 zugeordnet. Der ersten sekundären Adresse 612, den zusätzlichen sekundären Adressen 616 und der endgültigen sekundären Adresse 614 sind ebenfalls sekundäre Adresscodes 622, 626, 624 zugeordnet. Nach Feststellung einer Gefährdung kann die feststellende Maschine einfach einen Änderungscode senden, um zur nächsten nachfolgenden Adresse zu wechseln. Beispielsweise führt die erste Gefährdung zum Wechsel von der VPN-Hauptadresse 610 zur ersten sekundären Adresse 612. Die zweite Gefährdung würde in gleicher Weise eine Verschiebung nach unten in der Reihenfolge der angeforderten Adressenliste verursachen, bis die endgültige sekundäre Adresse 614 erreicht ist, nach welcher wieder die VPN-Hauptadresse 610 die nächstgewählte Adresse sein würde.

[0044] In einer alternativen Ausführung kann die feststellende Maschine einen Änderungscode senden, welcher entsprechend der Adresse, zu der gewechselt wird, den Haupt- oder den sekundären Adresscode 620, 622, 626, 624 angibt. Der angegebene Änderungscode kann aus einem Satz von verfügbaren Adresscodes zufällig festgelegt werden. Da beide Knoten die gleiche Beziehung von Adresscodes zu IP-Adressen haben, wird eine identische Änderung der entsprechenden IP-Adressen 610, 612, 616, 614 an beiden Knoten vorgenommen.

[0045] Es ist von Vorteil, dass diese gleichen Algorithmustypen verwendet werden können, um eine Auswahl aus

einem Satz verwendbarer Chiffrierschlüssel oder Verschlüsselungsalgorithmen zu treffen, wie jeweils in Fig. 6B und Fig. 6C dargestellt. Es sei darauf hingewiesen, dass alternativ Chiffrierschlüssel zufällig und sich nicht wiederholend erzeugt werden können, sodass jedesmal, wenn ein Schlüssel verwendet wird, ein neuer Schlüssel erzeugt wird, um diesen zu ersetzen. Neue Schlüssel können sofort nach Erzeugung ausgetauscht werden, wenn die Sicherheit des VPN-Tunnels gewährleistet ist.

[0046] Bei einer Änderung des VPN-Tunnels 528 müssen nicht alle Konfigurationsaspekte geändert werden. In einer alternativen Ausführung können beispielsweise die Adressen geändert werden, während die Chiffrierschlüssel und Verschlüsselungsverfahren unverändert bleiben. Der höchste Sicherheitsvorteil wird jedoch erreicht, wenn alle Konfigurationsdaten für den VPN-Tunnel 528 geändert werden.

[0047] Die bisherige Diskussion hat die Arbeitsweise und die Anwendung der vorliegenden Erfindung deutlich gemacht. Mit Bezug auf die obige Beschreibung sollte erkannt werden, dass, auch wenn Ausführungen bestimmten Materials offengelegt wurden, diese ermöglichenden Ausführungen beispielhaft sind, und dass die optimalen Beziehungen der erfindungsgemäßen Komponenten Variationen in Zusammensetzung, Form, Funktion und Arbeitsweise beinhalten, was für Fachleute anhand der vorliegenden Darlegung offensichtlich ist. Alle zu den in dieser Spezifikation enthaltenen Zeichnungen äquivalenten Zusammenhänge sollen durch die vorliegende Erfindung abgedeckt sein.

[0048] Folglich wird die vorhergehende Offenlegung als beispielhafte Darstellung der Grundzüge der Erfindung angesehen. Da sich für den Fachmann leicht zahlreiche Veränderungen ergeben, ist nicht beabsichtigt, die Erfindung genau auf die beschriebene und dargestellte Bauweise und den beschriebenen und dargestellten Betrieb zu beschränken, so dass auf alle geeigneten Veränderungen und Entsprechungen, die im Geltungsbereich der Erfindung liegen, zurückgegriffen werden kann.

#### Patentansprüche

1. Getunneltes Netzsystem, welches beinhaltet:
  - einen ersten getunnelten Knoten mit einem ersten Satz von Tunnelungskonfigurationsdaten und mindestens einem ersten zugehörigen Sicherungskonfigurationselement;
  - einen zweiten getunnelten Knoten mit einem zweiten Satz von Tunnelungskonfigurationsdaten und mindestens einem zweiten zugehörigen Sicherungskonfigurationselement; und
  - ein getunneltes Netzsystem zwischen dem ersten getunnelten Knoten und dem zweiten getunnelten Knoten,
- wobei der erste getunnelte Knoten betrieben werden kann, um ein ausgewähltes erstes Sicherungskonfigurationselement aus dem Satz der ersten Sicherungskonfigurationselemente auszuwählen, um einen Änderungscode zum zweiten getunnelten Knoten zu senden, und um das ausgewählte erste Sicherungskonfigurationselement zum Verhandeln eines getunnelten Sicherungsnetzes mit dem zweiten getunnelten Knoten in Betrieb zu nehmen, und
- der zweite getunnelte Knoten zum Empfang und zur Interpretation des Änderungscode betrieben werden kann, um ein ausgewähltes zweites Sicherungskonfigurationselement aus dem Satz der zweiten Sicherungskonfigurationselemente auszuwählen, und um das ausgewählte zweite Sicherungskonfigurationselement zum Verhandeln des getunnelten Sicherungsnetzes mit



dem ersten getunnelten Knoten zu verwenden.

2. Getunneltes Netzsystem gemäß Anspruch 1, wobei der erste getunnelte Knoten weiterhin betrieben werden kann, um Gefährdungen des getunnelten Netzes festzustellen und den Änderungscode bei Feststellung einer Gefährdung des getunnelten Netzes zu senden.

3. Getunneltes Netzsystem gemäß Anspruch 2, wobei die Gefährdung eine Sicherheitsgefährdung ist.

4. Getunneltes Netzsystem gemäß Anspruch 2, wobei der zweite getunnelte Knoten betrieben werden kann, um beim Empfang des Änderungscode einen Empfangsbestätigungscode zum ersten getunnelten Knoten zu senden, und wobei der erste getunnelte Knoten betrieben werden kann, um vor dem Versuch der Verhandlung des getunnelten Sicherungsnetzes den Empfangsbestätigungscode vom zweiten getunnelten Knoten zu empfangen.

5. Getunneltes Netzsystem gemäß Anspruch 2, wobei der erste Satz Netzkonfigurationsdaten eine Quelladresse, eine Zieladresse, mindestens einen ersten Chiffrierschlüssel und ein Verschlüsselungsverfahren umfasst, und wobei der zweite Satz Netzkonfigurationsdaten die Quelladresse, die Zieladresse, mindestens einen zweiten Chiffrierschlüssel und das Verschlüsselungsverfahren umfasst.

6. Getunneltes Netzsystem gemäß Anspruch 5, wobei das erste Sicherungskonfigurationselement mindestens ein Element aus folgender Menge: einer Adresse, einem Chiffrierschlüssel und einem Verschlüsselungsverfahren ist, und wobei das zweite Sicherungskonfigurationselement mindestens ein Element aus folgender Menge: einer Adresse, einem Chiffrierschlüssel und einem Verschlüsselungsverfahren ist.

7. Getunneltes Netzsystem gemäß Anspruch 2, wobei der erste getunnelte Knoten betrieben werden kann, um nach dem Senden des Änderungscode den Netztunnel aufzugeben, und der zweite getunnelte Knoten betrieben werden kann, um nach dem Empfang des Änderungscode den Netztunnel aufzugeben.

8. Getunneltes Netzsystem gemäß Anspruch 2, wobei der erste getunnelte Knoten betrieben werden kann, um nach dem Senden des Änderungscode falsche Daten durch den Netztunnel zu übertragen, und der zweite getunnelte Knoten betrieben werden kann, um nach dem Empfang des Änderungscode falsche Daten durch den Netztunnel zu übertragen.

9. Getunneltes Netzsystem gemäß Anspruch 4, das weiterhin umfasst:

mindestens einen zusätzlichen getunnelten Knoten mit einem zusätzlichen Satz von Tunnelungskonfigurationsdaten und mindestens ein zugehöriges zusätzliches Sicherungskonfigurationselement,

wobei der Netztunnel weiterhin den ersten getunnelten Knoten und den zweiten getunnelten Knoten mit dem zusätzlichen getunnelten Knoten verbindet, und

der zusätzliche getunnelte Knoten zum Empfang und zur Interpretation des Änderungscode betrieben werden kann, um ein ausgewähltes zusätzliches Sicherungskonfigurationselement aus dem Satz zusätzlicher Sicherungskonfigurationselemente auszuwählen, und

damit zu beginnen, das ausgewählte zusätzliche Sicherungskonfigurationselement zum Verhandeln des getunnelten Sicherungsnetzes mit dem ersten getunnelten Knoten und dem zweiten getunnelten Knoten zu verwenden, wobei der erste getunnelte Knoten weiterhin betrieben wird, um vor dem Versuch der Verhandlung des getunnelten Sicherungsnetzes den Empfangsbestätigungscode vom zusätzlichen getunnelten Knoten zu

empfangen.

10. Verfahren in einem getunnelten Netzsystem mit einem ersten getunnelten Knoten und einem zweiten getunnelten Knoten, das die Schritte umfasst:

die Zuordnung eines ersten Satzes von Tunnelungskonfigurationsdaten und mindestens eines ersten Sicherungskonfigurationselements zu dem ersten getunnelten Knoten;

die Zuordnung eines zweiten Satzes von Tunnelungskonfigurationsdaten und mindestens eines zweiten Sicherungskonfigurationselements zu dem zweiten getunnelten Knoten;

die Auswahl mindestens eines ausgewählten ersten Sicherungselements aus mindestens einem ersten Sicherungskonfigurationselement durch den ersten getunnelten Knoten;

die Auswahl mindestens eines ausgewählten zweiten Sicherungselements aus mindestens einem zweiten Sicherungskonfigurationselement durch den zweiten getunnelten Knoten; und

die Verhandlung eines zweiten getunnelten Netzsystems durch den ersten getunnelten Knoten und den zweiten getunnelten Knoten durch Verwenden mindestens des ausgewählten ersten Sicherungselements und mindestens des ausgewählten zweiten Sicherungselements.

11. Verfahren gemäß Anspruch 10, das weiterhin die Schritte umfasst:

das Feststellen einer potentiellen Gefährdung innerhalb des getunnelten Netzsystems beim ersten getunnelten Knoten; und

die Warnung des zweiten getunnelten Knotens vor der potentiellen Gefährdung durch den ersten getunnelten Knoten.

12. Verfahren gemäß Anspruch 11, wobei die potentielle Gefährdung eine potentielle Sicherheitsgefährdung ist.

13. Verfahren gemäß Anspruch 10, das weiterhin die Schritte umfasst:

das Senden eines Empfangsbestätigungscode vom zweiten getunnelten Knoten zum ersten getunnelten Knoten beim Empfang des Änderungscode; und den Empfang des vom zweiten getunnelten Knoten gesendeten Empfangsbestätigungscode durch den ersten getunnelten Knoten vor dem Versuch der Verhandlung des zweiten getunnelten Netzsystems.

14. Verfahren gemäß Anspruch 10, das weiterhin die Schritte umfasst:

die Aufgabe des Netztunnels durch den ersten getunnelten Knoten nach dem Senden des Änderungscode; und

die Aufgabe des Netztunnels durch den zweiten getunnelten Knoten nach dem Empfang des Änderungscode.

15. Verfahren gemäß Anspruch 10, das weiterhin die Schritte umfasst:

das Senden falscher Daten durch den Netztunnel durch den ersten getunnelten Knoten nach dem Senden des Änderungscode; und

das Senden falscher Daten durch den Netztunnel durch den zweiten getunnelten Knoten nach dem Empfang des Änderungscode.

16. Getunneltes Netzsystem, das umfasst:

einen ersten getunnelten Knoten mit einem ersten Satz von Tunnelungskonfigurationsdaten und mindestens einem ersten zugehörigen Sicherungskonfigurationselement;

einen zweiten getunnelten Knoten mit einem zweiten



Satz von Tunnelungskonfigurationsdaten und mindestens einem zweiten zugehörigen Sicherungskonfigurationselement;  
 einen Hauptnetzunnel zwischen dem ersten getunnelten Knoten und dem zweiten getunnelten Knoten, verbunden mit dem ersten Satz von Tunnelungskonfigurationsdaten und dem zweiten Satz von Tunnelungskonfigurationsdaten; und  
 mindestens einen Sicherungstunnel zwischen dem ersten getunnelten Knoten und dem zweiten getunnelten Knoten, verbunden mit mindestens einem ersten Sicherungskonfigurationselement, und mit mindestens einem zweiten Sicherungskonfigurationselement, wobei der erste getunnelte Knoten betrieben werden kann, um einen Änderungscode zum zweiten getunnelten Knoten zu senden, und um den Sicherungstunnel zur Kommunikation mit dem zweiten getunnelten Knoten in Betrieb zu nehmen, und der zweite getunnelte Knoten betrieben werden kann, um einen Änderungscode zu empfangen, und um den Sicherungstunnel zur Kommunikation mit dem ersten getunnelten Knoten in Betrieb zu nehmen.  
 17. Getunneltes Netzsystem gemäß Anspruch 16, wobei der erste Knoten weiterhin betrieben werden kann, um eine Gefährdung des Hauptnetzunnels festzustellen und um nach Feststellung der Gefährdung den Änderungscode zu senden.  
 18. Getunneltes Netzsystem gemäß Anspruch 17, wobei die Gefährdung eine Sicherheitsgefährdung ist.  
 19. Getunneltes Netzsystem gemäß Anspruch 16, wobei der zweite getunnelte Knoten betrieben werden kann, um nach dem Empfang des Änderungscode einen Empfangsbestätigungscode zum ersten getunnelten Knoten zu senden, und wobei der erste getunnelte Knoten betrieben werden kann, um vor der Verwendung des Sicherungstunnels einen Empfangsbestätigungscode vom zweiten getunnelten Knoten zu empfangen.  
 20. Getunneltes Netzsystem gemäß Anspruch 16, wobei der erste Satz von Netzkonfigurationsdaten eine Quelladresse, eine Zieladresse, mindestens einen ersten Chiffrierschlüssel und ein Verschlüsselungsverfahren umfasst, und wobei der zweite Satz von Netzkonfigurationsdaten die Quelladresse, die Zieladresse, mindestens einen zweiten Chiffrierschlüssel und das Verschlüsselungsverfahren umfasst.  
 21. Getunneltes Netzsystem gemäß Anspruch 16, wobei der erste getunnelte Knoten betrieben werden kann, um nach dem Senden des Änderungscode den Hauptnetzunnel aufzugeben, und der zweite getunnelte Knoten betrieben werden kann, um nach dem Empfang des Änderungscode den Hauptnetzunnel aufzugeben.  
 22. Getunneltes Netzsystem gemäß Anspruch 16, wobei der erste getunnelte Knoten betrieben werden kann, um nach dem Senden des Änderungscode falsche Daten über den Hauptnetzunnel zu senden, und der zweite getunnelte Knoten betrieben werden kann, um nach dem Empfang des Änderungscode falsche Daten über den Hauptnetzunnel zu senden.  
 23. Getunneltes Netzsystem gemäß Anspruch 19, das weiterhin umfasst:  
 mindestens einen zusätzlichen getunnelten Knoten mit einem zusätzlichen Satz von Tunnelungskonfigurationsdaten und mindestens einem zugehörigen zusätzlichen Sicherungskonfigurationselement, wobei der Hauptnetzunnel weiterhin den ersten getunnelten Knoten und den zweiten getunnelten Knoten mit dem zusätzlichen getunnelten Knoten unter Verwen-

dung des zusätzlichen Satzes von Tunnelungskonfigurationsdaten verbindet, und  
 wobei der Sicherungstunnel weiterhin den ersten getunnelten Knoten und den zweiten getunnelten Knoten mit dem zusätzlichen getunnelten Knoten unter Verwendung mindestens eines zusätzlichen Sicherungskonfigurationselementes verbindet, und der zusätzliche getunnelte Knoten betrieben werden kann, um den Änderungscode zu empfangen, den Empfangsbestätigungscode zum ersten getunnelten Knoten zu senden und den Sicherungstunnel für die Kommunikation mit dem ersten getunnelten Knoten und dem zweiten getunnelten Knoten in Betrieb zu nehmen, und  
 wobei der erste getunnelte Knoten weiterhin betrieben werden kann, um vor dem Verwenden des Sicherungstunnels den Empfangsbestätigungscode vom zusätzlichen getunnelten Knoten zu empfangen.  
 24. Knoten zu einem getunnelten Netzsystem, der umfasst:  
 einen Satz Tunnelungskonfigurationsdaten;  
 mindestens einen Satz Sicherungskonfigurationsdaten; und  
 einen getunnelten Netzendpunkt,  
 wobei der Knoten betrieben werden kann, um den Satz von Sicherungskonfigurationsdaten in Betrieb zu nehmen, um einen getunnelten Sicherungstunnel einzurichten.  
 25. Knoten gemäß Anspruch 24, wobei der Knoten betrieben werden kann, um Gefährdungen am getunnelten Netzendpunkt festzustellen und den Satz von Sicherungskonfigurationsdaten nach Feststellung einer Gefährdung in Betrieb zu nehmen.  
 26. Knoten gemäß Anspruch 25, wobei die Gefährdung eine Sicherheitsgefährdung ist.  
 27. Knoten gemäß Anspruch 25, wobei der Satz von Tunnelungskonfigurationsdaten eine Quelladresse, eine Zieladresse, mindestens einen ersten Chiffrierschlüssel und ein Verschlüsselungsverfahren umfasst.  
 28. Knoten gemäß Anspruch 25, wobei der Knoten betrieben werden kann, um nach dem Einrichten des getunnelten Sicherungstunnels den getunnelten Netzendpunkt aufzugeben.  
 29. Knoten gemäß Anspruch 25, wobei der Knoten betrieben werden kann, um nach Einrichtung des getunnelten Sicherungstunnels falsche Daten vom getunnelten Netzendpunkt zu senden.  
 30. Computerlesbarer Datenträger, auf dem ein Computerprogramm gespeichert ist, das umfasst:  
 einen Konfigurationsspeichercode mit einem Satz von Codes, die einen Knoten anweisen, einen Satz von Tunnelungskonfigurationsdaten abzuspeichern;  
 einen Sicherungskonfigurationsspeichercode mit einem Satz von Codes, die den Knoten anweisen, einen Satz von Tunnelungskonfiguration-Sicherungsdaten abzuspeichern;  
 einen getunnelten Netzendpunktecode mit einem Satz von Codes, die den Knoten anweisen, einen getunnelten Netzendpunkt unter Verwendung eines Satzes von Tunnelungskonfigurationsdaten einzurichten; und  
 einen Umschaltcode mit einem Satz von Codes, die den Knoten anweisen, einen getunnelten Sicherungstunnel unter Verwendung eines Satzes von Tunnelungskonfiguration-Sicherungsdaten einzurichten.  
 31. Computerlesbarer Datenträger gemäß Anspruch 30, auf dem zusätzlich ein Computerprogramm gespeichert ist, das umfasst:  
 einen Detektionscode mit einem Satz von Codes, die



den Knoten anweisen, eine Gefährdung des getunnel-  
ten Netzendpunkts festzustellen; und  
einen Warncode mit einem Satz von Codes, die den  
Knoten anweisen, mit der Ausführung des Umschalt-  
codes nach Feststellung der Gefährdung zu beginnen. 5  
32. Computerlesbarer Datenträger gemäß Anspruch  
31, wobei der Satz von Tunnelungskonfigurationsdaten  
eine Quelladresse, eine Zieladresse, mindestens einen  
ersten Chiffrierschlüssel und ein Verschlüsselungsver-  
fahren umfasst. 10  
33. Computerlesbarer Datenträger gemäß Anspruch  
32, wobei die Gefährdung eine Sicherheitsgefährdung  
ist.  
34. Computerlesbarer Datenträger gemäß Anspruch  
32, wobei der Umschaltcode darüber hinaus betrieben 15  
werden kann, um den Knoten anzuweisen, nach Ein-  
richtung des getunnelten Sicherungsnetzendpunktes  
den getunnelten Netzendpunkt aufzugeben.  
35. Computerlesbarer Datenträger gemäß Anspruch  
32, wobei der Umschaltcode darüber hinaus betrieben 20  
werden kann, um den Knoten anzuweisen, nach Ein-  
richtung des getunnelten Sicherungsnetzendpunktes  
falsche Daten von dem getunnelten Netzendpunkt zu  
senden. 25

---

Hierzu 7 Seite(n) Zeichnungen

---

30

35

40

45

50

55

60

65



- Leerseite -



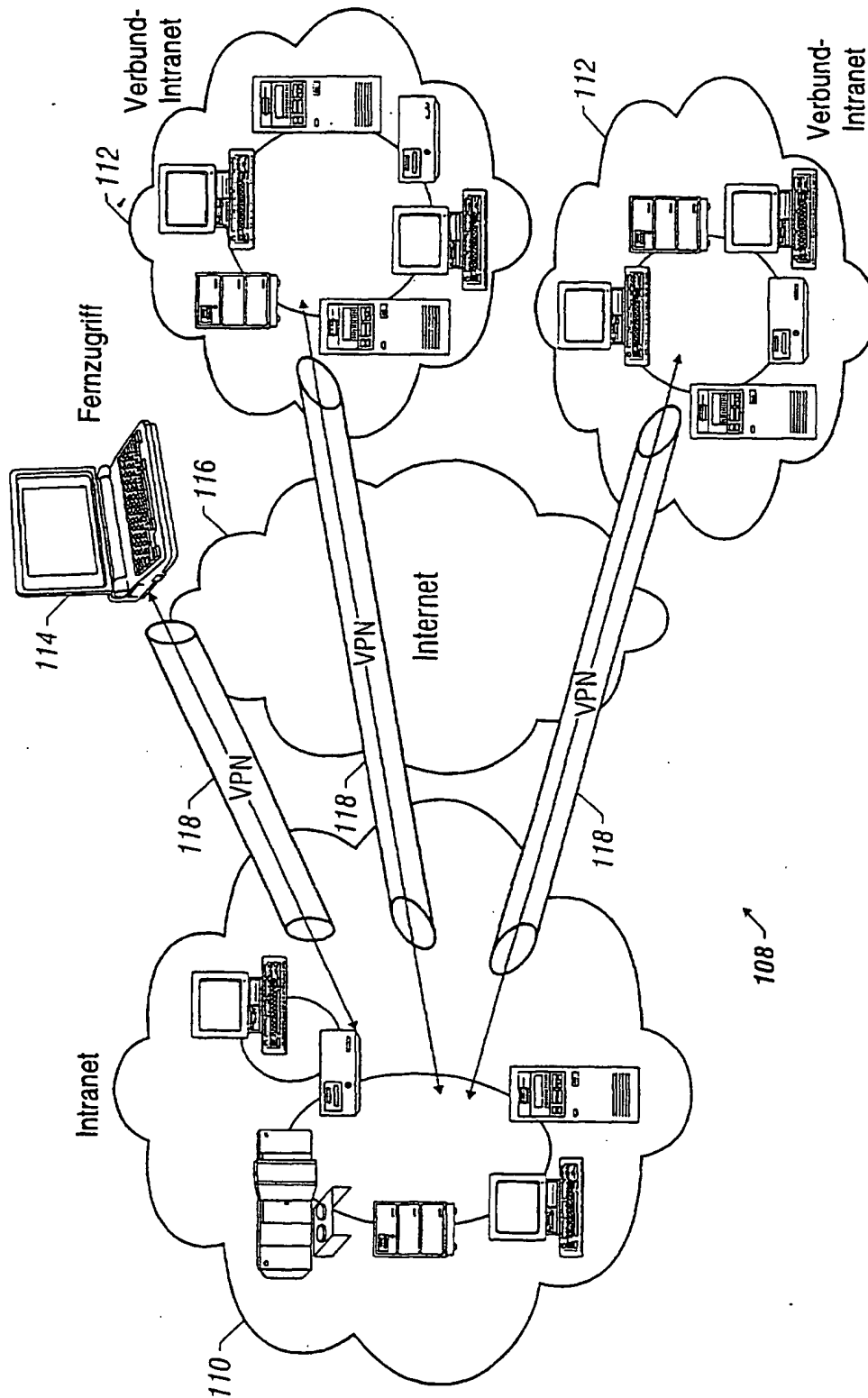


FIG. 1



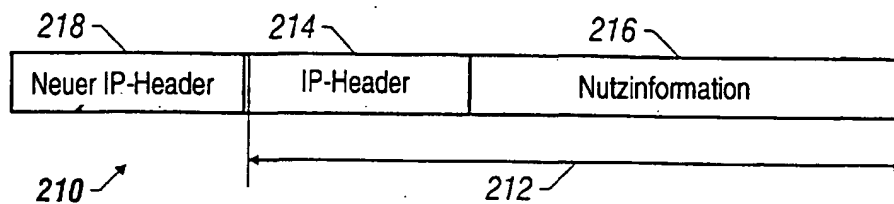


FIG. 2

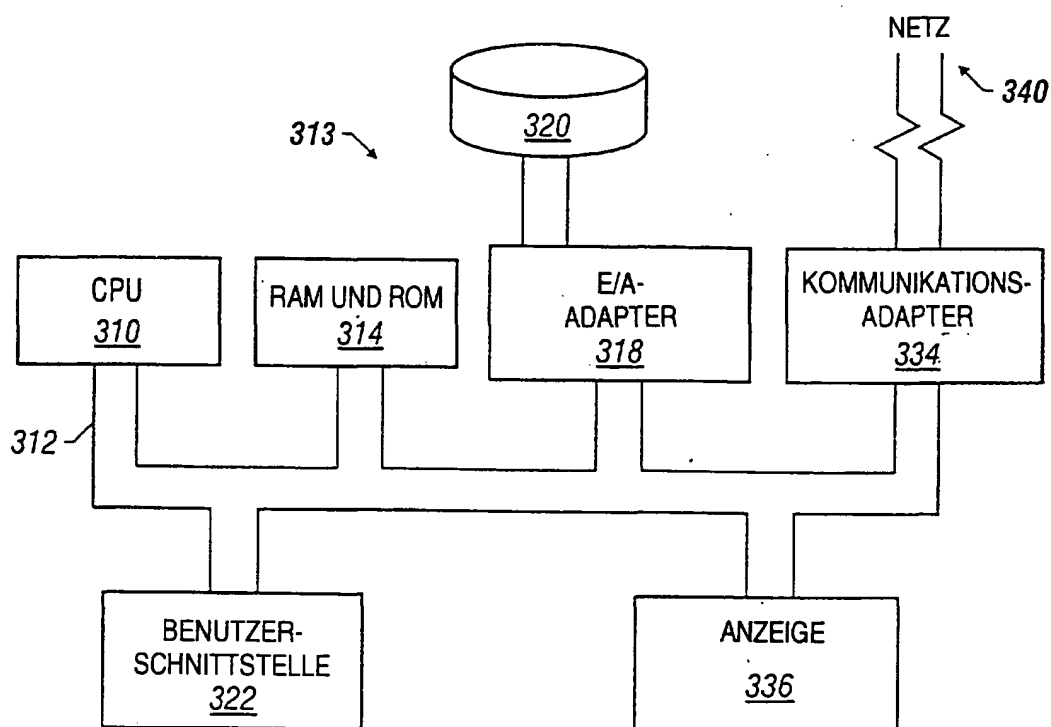


FIG. 3



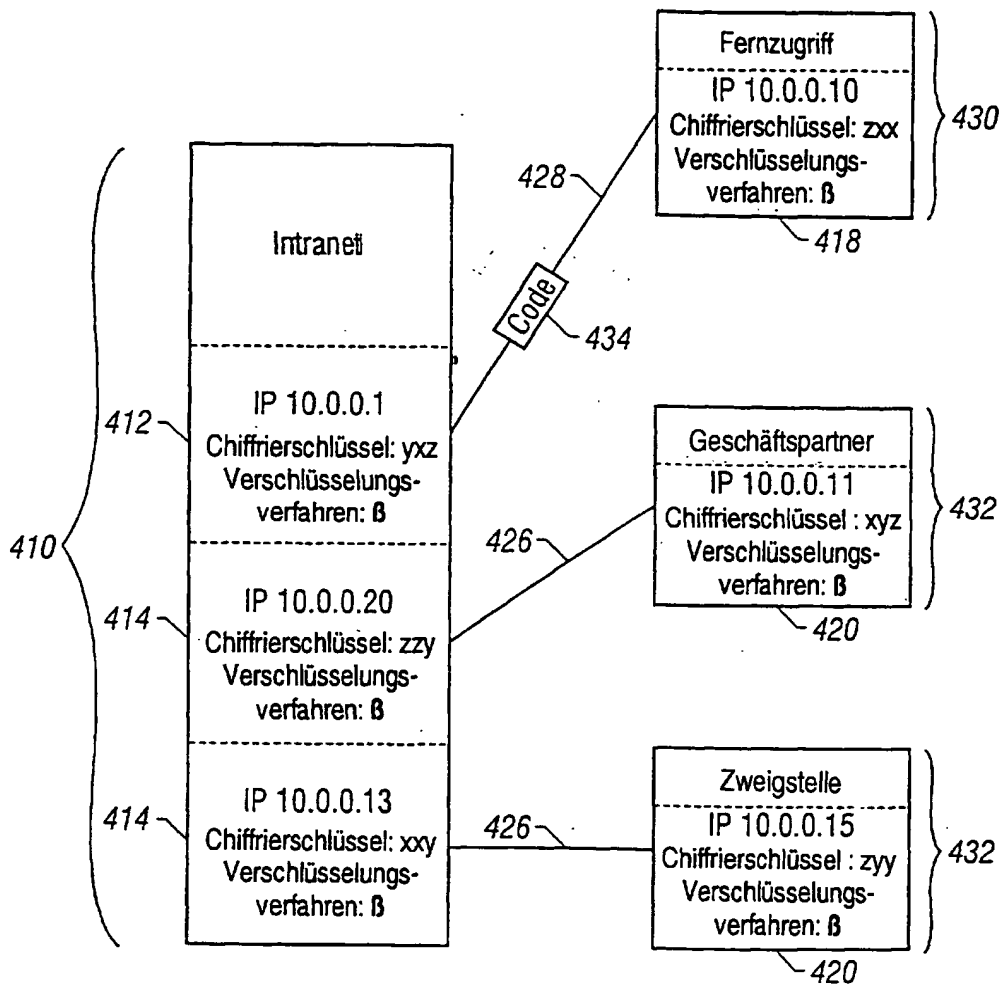


FIG. 4



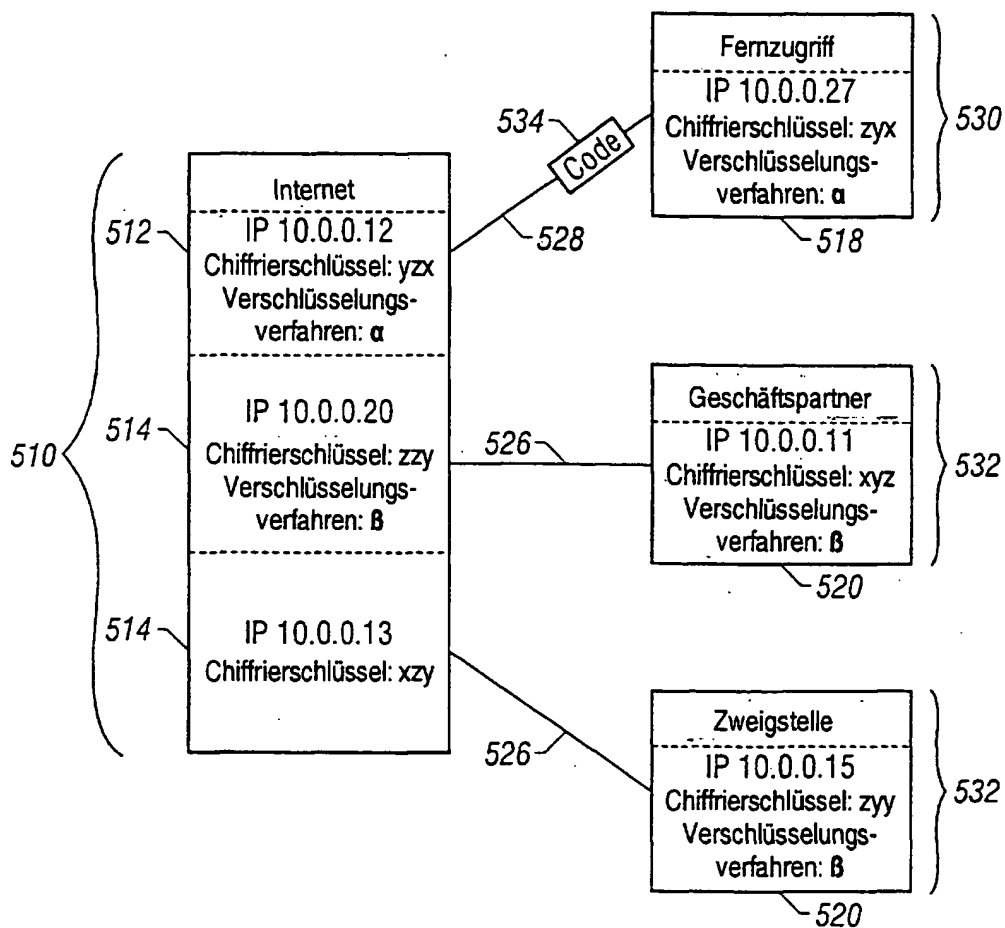


FIG. 5



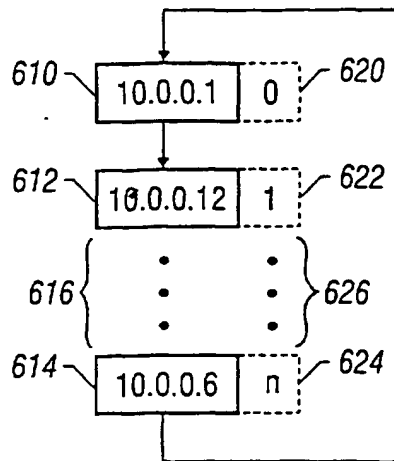


FIG. 6A

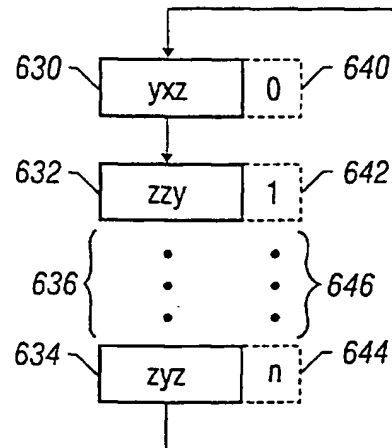


FIG. 6B

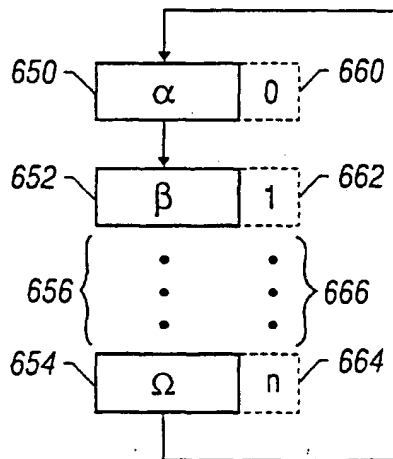


FIG. 6C



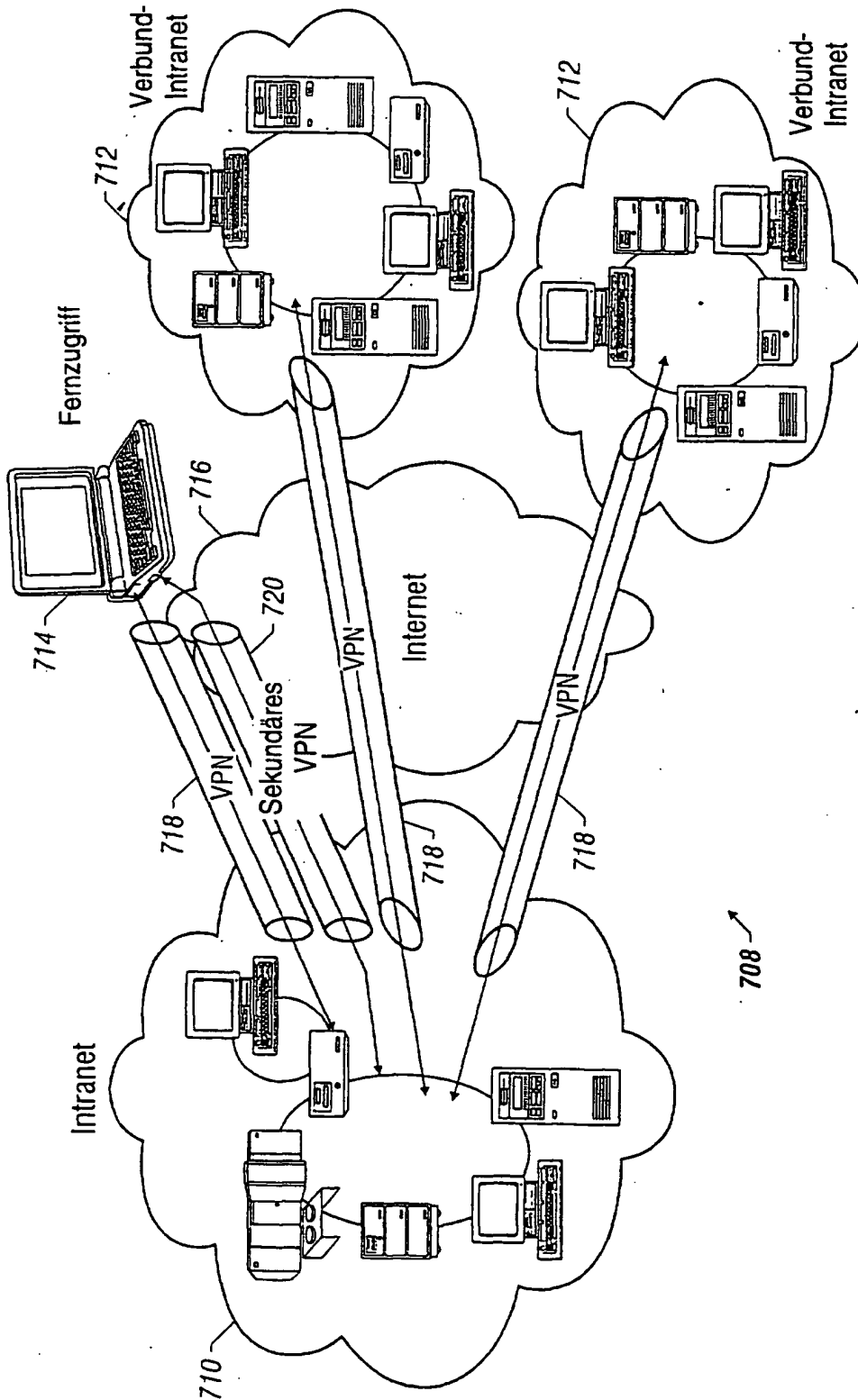


FIG. 7



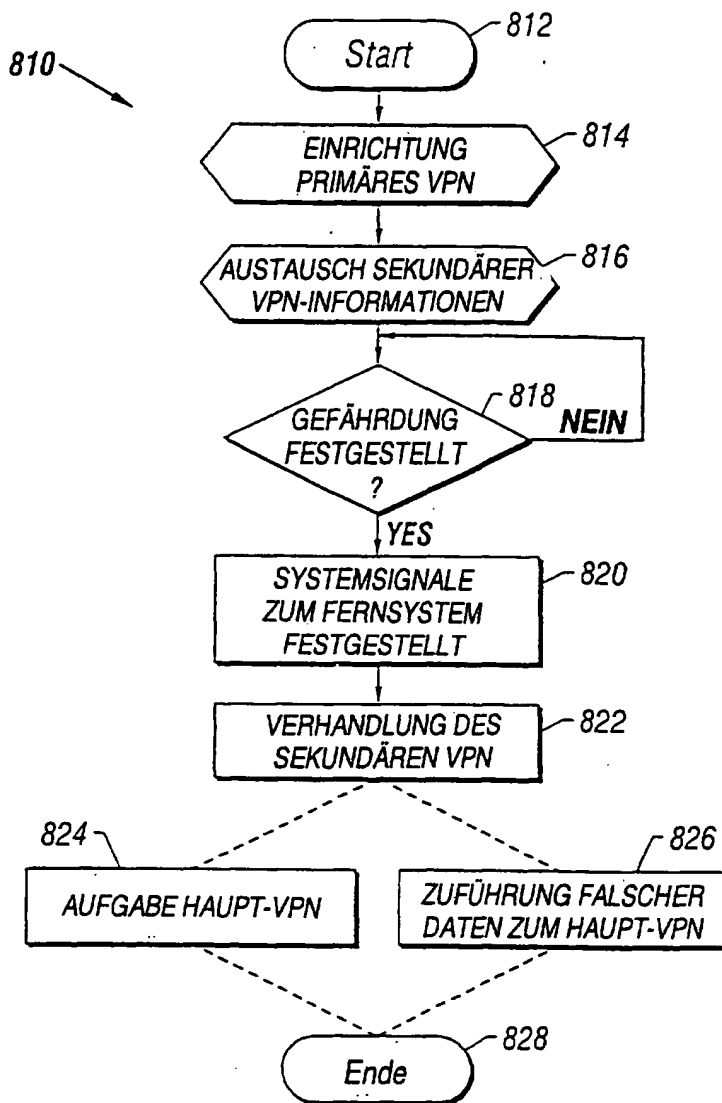


FIG. 8